Санкт-Петербургский государственный университет

Математико-механический факультет
Кафедра высшей алгебры и теории чисел

Балашов Александр Дмитриевич

Числа Кармайкла высших порядков

Дипломная работа

Научный руководитель:
д. ф.-м. н., профессор Всемирнов М. А.

Рецензент:
к. ф.-м. н., научный сотрудник Пастор А. В.

Санкт-Петербург
2017

SAINT-PETERSBURG STATE UNIVERSITY

Faculty of Mathematics and Mechanics
Department of algebra and number theory

Balashov Alexander

Higher order Carmichael numbers

Graduation Thesis

Scientific supervisor:
professor Maxim Vsemirnov

Reviewer:
research officer Aleksey Pastor

Saint-Petersburg
2017

Оглавление

Введение

Целью данной работы является оценка количества простых делителей для одного из обобщений чисел Кармайкла. Таким образом можно выявить следующие задачи:

1. Определить числа Кармайкла и используемые обощения чисел Кармайкла.

2. Показать связь между обощениями чисел Кармайкла.

3. Доказать теоремы для оценки количества простых делителей.

Объектом изучения являются числа Кармайкла порядка m и числа, соответсвующие главным идеалами Кармайкла в любом расширении Q степени m. Предмет изучения — количество делителей у таких чисел.

В первой главе вводятся определения и формулируются известные теоремы про числа Кармайкла и их обощения. Определения обобщений берутся из работ Хоува [4] и Стила [6]. Во второй главе показаны связи между данными определениями. В третьей главе доказываются теоремы о количестве простых делителей чисел Кармайкла и их обобщений. Метод доказательства основан на идее, использованной в работе Етеревского и Всемирнова [3].

1. Основные определения

Классические числа Кармайкла хорошо изучены в теории чисел. Доказано, что чисел Кармайкла бесконечно много, более того, существует оценка снизу на количество чисел Кармайкла не превышающих заданное число [1], также известен алгоритм генерации больших чисел Кармайкла с помощью конструкции Эрдеша [1].

***Определение* 1** (число Кармайкла)**.**
Положительное составное число n называется числом Кармайкла если $a^n \equiv a \pmod{n}$ для любого числа a. Другими словами, числа Кармайкла — в точности псевдопростые числа для любой базы.

Существует несколько видов обобщений чисел Кармайкла. Мы будем использовать следующие: Хоув заменил кольцо $\mathbb{Z}/n\mathbb{Z}$ на произвольную $\mathbb{Z}/n\mathbb{Z}$-алгебру, Стил обобщил тест на простоту над $\mathbb{Q}$ на тест над произвольным конечным расширением $\mathbb{Q}$.

***Определение* 2** (число Кармайкла порядка m, [4])**.**
Составное число n называется числом Кармайкла порядка m, если для любой $(\mathbb{Z}/n\mathbb{Z})$-алгебры, порожденной m элементами как $(\mathbb{Z}/n\mathbb{Z})$-модуль, отображение $x \mapsto x^n$ является эндоморфизмом.

Для простого числа p у любой $\mathbb{Z}/p\mathbb{Z}$-алгебры отображение $x \mapsto x^p$ является эндоморфизмом [4].

Это определение тяжело использовать, поэтому мы будем пользоваться аналогом критерия Корсельта:

***Теорема* 1** (критерий Корсельта для порядка m, [4])**.**
Составное число n является числом Кармайкла порядка m тогда и только тогда, когда

1. *n свободно от квадратов;*
2. *для любого простого делителя p числа n и для всех $i < m$ существует $s > 0$, такое, что $n \equiv p^s \pmod{p^i - 1}$.*

Также введем определение строгих чисел Кармайкла порядка m. Это подмножество чисел Кармайкла порядка m, но оно более удобно для изучения.

***Определение* 3** (строгие числа Кармайкла порядка m, [4])**.**
Составное число n является строгим числом Кармайкла порядка m тогда и только тогда, когда

1. *n свободно от квадратов;*
2. *для любого простого делителя p числа n и для всех $i < d$ выполнено сравнение $n \equiv 1 \pmod{p^i - 1}$.*

Аналогом теста на простоту в поле K с кольцом целых $\mathcal{O}_K$ является проверка равенств

$$\forall \alpha \in \mathcal{O}_K \quad \alpha^{\mathbf{Nm}(\rho)} \equiv \alpha \pmod{\rho}$$

.

***Определение* 4** (идеал Кармайкла в расширением K, [6])**.**
Пусть $K/\mathbb{Q}$ — конечное расширение, n — составной идеал в $\mathcal{O}_K$, n — идеал Кармайкла в K, если

$$\forall \alpha \in \mathcal{O}_K \quad \alpha^{\boldsymbol{Nm}(n)} \equiv \alpha \ (\boldsymbol{mod}\ n)\,.$$

В конкретном расширении Галуа K идеалов Кармайкла достаточно много, например любое простое число p, которое расщепляется в расширении на произведение различных простых идеалов $(p) = p_1 \cdots p_e$, p_i различны, $e > 1$, будет идеалом Кармайкла над K.

$$\mathbf{Nm}(p) = p^d, \quad d = [K : \mathbb{Q}]$$

$$\mathbf{Nm}(p_i) = p^f, \quad p^f - 1 \mid p^d - 1, \text{ где } d = f \cdot e$$

Имеет смысл говорить о таких натуральных числах n, которые соответствуют главным идеалам Кармайкла над K для любого K, такого, что степень расширения $K/\mathbb{Q}$ равна d и $\gcd(Disc(K), n) = 1$. Для таких чисел существует следующий критерий.

***Теорема* 2** (критерий Корсельта для расширений, [6])**.**
Составное натуральное число n порождает идеал Кармайкла в любом расширении K степени d, для которого $\gcd(Disc(K), n) = 1$, *тогда и только тогда, когда*

1. *n свободно от квадратов;*

2. *если $p \mid n$, то $\forall\ i \leq d \quad p^i - 1 \mid n^d - 1$.*

2. Связь обобщений чисел Кармайкла

Мы будем обозначать множество чисел Кармайкла порядка m как C_m; множество строгих чисел Кармайкла порядка m как RC_m; чисел, порождающих идеал Кармайкла в любом расширении порядка m как EC_m. Между этими множествами есть тривиальные вложения:

$$\begin{array}{ccccccc} C_1 & \supset & C_2 & \supset & C_3 & \dots \\ \| & & \cup & & \cup & \\ RC_1 & \supset & RC_2 & \supset & RC_3 & \dots \\ \| & & \cap & & \cap & \\ EC_1 & & EC_2 & & EC_3 & \dots \end{array}$$

Причем вложений $EC_m \not\subset EC_{m-1}$ нет, например, число $11 \cdot 19 \cdot 41 = 8569 \in EC_2 \setminus EC_1$.

3. Оценки на делители

Для классических чисел Кармайкла количество простых делителей больше или равно 3(см. [5]).
Обозначим

$$\zeta_m = \sum_{i=1}^{m} \phi(i), \tag{1}$$

где $\phi(x)$ — функция Эйлера.

Для чисел Кармайкла порядка m количество делителей не меньше $\min(m+2, \zeta_m + 1)$ (см. [3]).

Для чисел из EC_m докажем две аналогичные оценки на простые делители.

Теорема 3.
Число из EC_m имеет по крайней мере 3 простых делителя.

Теорема 4.
Число из EC_m имеет по крайней мере $\left\lfloor \frac{\zeta_m}{m} \right\rfloor + 1$ делителей.

Для величины определенной в (1) имеется асимптотическая оценка (см. [2]):

$$\zeta_m \geq \frac{3}{\pi^2} \cdot m^2 - \frac{1}{2} \cdot m \ln m - \left(\frac{\gamma}{2} + \frac{5}{8}\right) \cdot m - 1, \tag{2}$$

где $\gamma = 0.57721\ldots$ — константа Эйлера. Соответственно, ζ_m/m имеет линейную асимптотику. Для $m < 9$ первая оценка (теорема 3) не слабее второй, следовательно для $m \leq 8$ количество простых делителей больше 2, для $m \geq 9$ простых делителей больше 3.

Доказательство теоремы 3. Пусть N $\in EC_m$, $N = p \cdot q$, p — наибольший простой делитель N, число N имеет s простых делителей. Тогда $N^m \equiv 1 \pmod{p^m - 1}$, $N > p$, следовательно,

$$\exists k > 1 : \ N^m - 1 = k \cdot (p^m - 1).$$

Получаем

$$p^m(k - q^m) = k - 1.$$

Таким образом, $k > p^m$.

$$(p^s)^m > N^m = k \cdot (p^m - 1) + 1 = k \cdot p^m - k + 1.$$

Так как

$$k \cdot p^m - k + 1 = k \cdot (p^m - 1) + 1 \geq (p^m + 1) \cdot (p^m - 1) + 1 = p^{2 \cdot m},$$

получаем

$$p^{s \cdot m} > p^{2 \cdot m}$$

Следовательно, количество s простых делителей больше 2. □

Пусть

$$F_m(x) = \prod_{i=1}^{m} \Phi_i(x), \tag{3}$$

где Φ_i — i-ый круговой многочлен.

***Лемма* 1** ([3])**.**
Для F_m и любого натурального n верно следующее:

1. $lcm(n-1, n^2-1, \ldots, n^m-1) = F_m(n)$;
2. $F_m(n) > (n-1)^{\zeta_m}$, *где число ζ_m определено в (1).*

Доказательство теоремы 4. Пусть $\mathrm{N} \in EC_m$, $N = p \cdot q$, p — наибольший простой делитель N, число N имеет s делителей. Тогда $N^m \equiv 1 \pmod{p^i - 1}, 0 < i \leq m$, следовательно

$$N^m \equiv 1 \pmod{lcm(p-1, p^2-1, \ldots, p^m-1)}.$$

Значит,

$$\exists k > 1 : \; N^m - 1 = k \cdot lcm(p-1, p^2-1, \ldots, p^m-1).$$

Так как у N как минимум 3 делителя, соответственно $s > 2$, то

$$N < p \cdot (p-2)^{s-1} = (p^2 - 2p) \cdot (p-2)^{s-2} < (p-1)^2 \cdot (p-1)^{s-2}.$$

Получаем

$$(p-1)^s > N = p \cdot q \text{ и по Лемме 1}$$

$$(p-1)^{m \cdot s} > N^m = k \cdot F_m(p) + 1 > (p-1)^{\zeta_m} \cdot k + 1,$$

то есть

$$(p-1)^{m \cdot s} > (p-1)^{\zeta_m}.$$

Так как s — целое, то $s \geq \left\lfloor \frac{\zeta_m}{m} \right\rfloor + 1$. □

Заключение

В ходе работы были доказаны следующие теоремы для чисел, которые порождают идеалы Кармайкла в любом расширении порядка m.

Теорема.
Число из EC_m имеет по крайней мере 3 простых делителя.

Теорема.
Число из EC_m имеет по крайней мере $\left\lfloor \frac{\zeta_m}{m} \right\rfloor + 1$ делителей.

Список литературы

[1] Alford W. R., Granville A., Pomerance C. There are infinitely many Carmichael numbers // Annals of Mathematics(2). — 1994. — Vol. 139. — P. 703—722.

[2] Dickson L.E. History of the Theory of Numbers. — Washington, 1919. — Vol. 1.

[3] Eterevsky O., Vsemirnov M. On the number of prime divisors of higher-order Carmichael numbers // Fibonacci Quarterly 42. — 2004. — Vol. 2. — P. 141–148.

[4] Howe E. W. Higher-order Carmichael numbers // Mathematics of Computation. — 2000. — Vol. 69. — P. 1711–1791.

[5] Koblitz N. A Course in Number Theory and Cryptography. — Springer-Verlag, 1994.

[6] Steele G. A. Carmichael numbers in number rings // Journal of Number Theory. — 2008. — Vol. 128. — P. 910–917.